MilesGuard

SWISS CYBERSECURITY

SOVEREIGN PLATFORM · LINUX + KUBERNETES

Take back control.
Your platform. Open source. In Switzerland.

One hardened foundation replaces dozens of cloud subscriptions: files, email, chat, video, ERP and AI on infrastructure you own, fully managed by MilesGuard. **Digital office, Security Operations Center (SOC), air-gap operation and drilled restores in one product.**

REPLACES SAAS SUBSCRIPTIONS LIKE

Microsoft 365 · Google Workspace · Slack · Teams · Zoom · Dropbox · Jira · Zendesk · Calendly · TeamViewer · 1Password · ChatGPT

TODAY		THIS PLATFORM
US hyperscalers · CLOUD Act · foreign law	→	Swiss law or your premises · air-gap capable
SaaS subscriptions · pricier every year	→	no licences, no telemetry · typically 30 to 50 percent cheaper · SOC included
Lock-in · exit costly and risky	→	everything as code in your Git · can be taken over even without MilesGuard

BASE TALOS LINUX + KUBERNETES · GITOPS FLUX CD · ZERO TRUST MTLS
HOSTING YOUR CHOICE: CLOUD, VPS OR ON-PREM · OPERATIONS FULLY MANAGED · CO-MANAGED · PURCHASE · CLOUD EXIT

40+	**100%**	**<15min**	**2×**
APPLICATIONS, ENABLE PER MODULE	OPEN SOURCE, NO BLACK BOX	AUTOMATIC SELF-HEALING	INDEPENDENT BACKUP PATHS, DRILLED

APPS

One login. Your complete digital office.

Over 40 applications behind one central single sign-on. You enable what you need; your own applications run alongside as standard containers. Plus the SOC's tooling (page 4).

Files & Office

6 APPS

- **Nextcloud**: files, calendar, contacts
- **Collabora**: office suite in the browser
- **Excalidraw**: whiteboard
- **Stirling-PDF**: PDF toolbox
- **Syncthing + Obsidian LiveSync**: file and note sync

replaces OneDrive · Dropbox · MS Office · Miro

Communication

7 APPS

- **Element / Matrix**: chat, federated, with video (Element Call)
- **Jitsi**: video conferencing
- **Stalwart**: your own mail server (SMTP/IMAP/JMAP)
- **Mastodon**: your own server in the Fediverse

replaces Slack · Teams · Zoom · Exchange

Business

8 APPS

- **ERPNext**: ERP: orders, inventory, accounting
- **Plane**: project management
- **Cal.com**: appointment scheduling
- **Zammad**: helpdesk & ticketing
- **Snipe-IT**: IT asset inventory
- **CISO Assistant**: governance, risk & compliance
- **Windmill + Temporal**: workflows & automation

replaces Jira · Calendly · Zendesk · Zapier

Local AI, no data leaving

4 APPS

- **Ollama + Open WebUI**: LLM chat on your own hardware; prompts and documents never leave the building
- **LibreTranslate**: translation
- **Whisper**: transcription (speech-to-text)

replaces ChatGPT subscriptions · DeepL

Access & Network

5 APPS

- **NetBird**: WireGuard VPN mesh
- **Guacamole**: RDP/SSH/VNC in the browser
- **RustDesk**: remote support
- **Vaultwarden**: password manager for teams
- **ALTCHA**: privacy-friendly captcha

replaces Tailscale · TeamViewer · 1Password

Operations, Media & Building

9 APPS

- **Homer / Glance**: portal & dashboard
- **Gatus**: status page
- **Coder**: cloud development environments
- **Headlamp**: Kubernetes UI
- **changedetection**: web monitoring
- **Jellyfin**: media
- **Home Assistant**: building automation
- **Frigate**: cameras/NVR with object detection

replaces Codespaces · Statuspage

ONE LOGIN

Keycloak single sign-on (OIDC) with hardware MFA (FIDO2/WebAuthn) in front of every application. Not a single route is reachable without authentication. Group-based permissions apply centrally, from file folders to the admin console.

INFRASTRUCTURE

The infrastructure in detail.

LAYER	COMPONENT	ROLE
OS	Talos Linux	immutable, API-only, LUKS2
GitOps	Flux CD	declarative desired state from Git
Network	Cilium	eBPF, kube-proxyless, WireGuard
Ingress	Traefik + Gateway API	TLS 1.3, HSTS, ForwardAuth
Identity	Keycloak + SPIRE	SSO (OIDC/FIDO2) + workload mTLS
Secrets	OpenBao + SOPS/age	secrets engine + Git encryption
Storage	Longhorn	replicated block storage (2 replicas)
Database	CloudNativePG	PostgreSQL operator, streaming backup
Backup	Velero + restic/Kopia	targets: SeaweedFS + Garage (S3, object lock)
Monitoring	VictoriaMetrics/Logs	metrics, logs, alerts (+ Vector)
Autoscaling	KEDA + KRR	load-driven, scale-to-zero, sizing
Registry / Git	Zot + Forgejo	air-gap source for images + code + CI
Policy	Kyverno	30+ admission policies, PSS restricted
Runtime security	Tetragon · Suricata	eBPF enforcement · IDS (+ CrowdSec IPS)
SIEM / XDR	Wazuh	XDR, log correlation
DFIR	Velociraptor + DFIR-IRIS	forensics, IR cases
SOAR / TI	Shuffle + MISP	playbooks, threat intel
Vulnerabilities	Greenbone · Trivy	network, image and SBOM scans

ARCHITECTURE: TIERS		EVICTION PROTECTION
T0	**Foundation**	GitOps engine, storage, database, workload identity; yields last.
T1	**Platform**	Network, ingress, certificates, monitoring, SSO, secrets, backup, security stack.
T2	**Apps**	40+ applications, individually enabled and paused; yield first under load.

Reference sizing

- ✓ **Production-ready from 4 nodes:** 3× control plane at 8 GiB (etcd quorum) + 1 worker at 16 GiB, grows with additional workers.
- ✓ **Provider-independent:** runs on any VPS provider or bare metal; switching providers is a documented standard procedure.
- ✓ **Bootstrap:** from empty nodes to a running cluster with one command (just install).
- ✓ **Storage contract:** every dataset has a class, a backup path and a documented loss impact; source data always replicated.

HARDENING · TLS ≥1.3 · HSTS · PKCE S256 · LUKS2 · WireGuard · mTLS required · PSS restricted · seccomp · readOnly-FS · non-root · SBOM CycloneDX · Cosign · CIS scans (kube-bench) · CVE scans (Trivy)

SECURITY & OPERATIONS

Defence in six layers. Operations, measured.

We regularly attack our own clusters and document the limits.

S1	**Immutable operating system**	Talos Linux · no SSH, no shell · managed only via signed API · LUKS2-encrypted
S2	**Network: default-deny**	every connection explicitly allowed, per service (Cilium) · WireGuard internally · TLS 1.3 + HSTS at the edge
S3	**Identity instead of IP addresses**	cryptographic identity per service (SPIFFE/SPIRE) · mTLS enforced
S4	**Admission control**	30+ rules (Kyverno) · signed images only · no root · strictest pod standard
S5	**Runtime monitoring**	kernel sensors (Tetragon) · IDS (Suricata) · IPS (CrowdSec) · honeypots with canary secrets
S6	**Detection & response**	complete SOC built in · detection, cases, forensics, threat intel

The built-in SOC

Elsewhere a project of its own, often six figures. Here, part of the platform:

- ✓ **Wazuh** — SIEM / XDR
- ✓ **DFIR-IRIS** — incident response cases
- ✓ **MISP** — threat intelligence
- ✓ **Shuffle** — SOAR automation
- ✓ **Velociraptor** — endpoint forensics
- ✓ **Greenbone + Trivy** — vulnerability scans
- ✓ **Gophish** — phishing simulation
- ✓ **MITRE Caldera** — attack emulation

OPERATIONS

GitOps	Every change is a commit · four-eyes via PR · CI gate before rollout · rollback via Git revert.
Self-healing	Stuck core components repair themselves in under 15 minutes, no intervention · dead-man heartbeats watch the watchers.
Backups	2 independent paths · S3 object lock · monthly restore drill (checksums) · etcd hourly.
Stress test	No outage of the core layers · recovery under 30 seconds · limits documented.
Monitoring	Metrics, logs, alerts (VictoriaMetrics) · status page (Gatus) · health check in 3 commands.
Updates	Weekly curated (Renovate) · CI-validated · version pinning instead of "latest" · CVE scans in the cluster.
Supply chain	SBOM (CycloneDX, Dependency-Track) · signed images only (Cosign) · air-gap mirror Forgejo + Zot.

COMPLIANCE · CIS Benchmark (kube-bench) · NIST SP 800-190 · nDSG · NIS2 · ISG · GRC tool included

Let's talk about your platform.

Free initial consultation. Fully managed (with managed security and an external CISO on request), co-managed: you run the apps, we run infrastructure and updates. Or purchase and step-by-step migration.

MilesGuard LLC
Bruggwiesenweg 18 · 9000 St. Gallen
info@milesguard.ch
+41 71 552 21 01 · milesguard.ch